IJIREEICE

ISSN (Online) 2321 – 2004
ISSN (Print) 2321 – 5526

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 3, Issue 12, December 2015

Advanced Secure Intrusion Detection System for MANET

Sayyed Musaddique[1], S.S.Hippargi[2], Attar Shuaib[3]

Department of Electronics and Telecommunication Engineering,

N.B. Navale Sinhgad College of Engineering and Technology, Solapur, India[1,2,3]

Abstract: In this project, we define solid privacy requirements regarding privacy-maintain routing in MANET. Then we propose an secure routing scheme to offer complete unlink ability and content un- observability for all types of packets. It is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that it can well protect user privacy against both inside and outside attackers. Privacy-preserving routing is crucial for some adhoc networks that require stronger privacy protection. A number of schemes have been proposed to protect privacy in adhoc networks. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes. In this paper, we define stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Then we propose an secure routing scheme to offer complete unlinkability and content unobservability for all types of packets. It is efficient as it uses a novel combination of group signature and ID-based encryption for route discovery. Security analysis demonstrates that it can well protect user privacy against both inside and outside attackers. We implement it on ns2, and evaluate its performance by comparing with AODV. The simulation results show that it not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes.

Keywords: MANET, AODV, MASK, Black hole Attack.

I. INTRODUCTION

Need of communication:
Communication is the process by which two or more people exchange ideas, facts, feelings, or impressions in ways that each gains a common understanding of the meaning, intent, and use of messages.

The term "communication" stems from the Latin word "communism" - meaning common. Thus, communication is a conscious attempt to share information, ideas, attitudes, and the like with others.

In short, it is the act of getting a sender of the message and a receiver of the message tuned together for a particular message, or a series of messages. For two or more people to engage in a common, co-operative effort, they must be able to communicate with each other. Thus, good communication consists of creating understanding of the message. In computerized technology, we need to transfer the data from one another without any problem like security and quality. To improve the communication in mobile adhoc network we need to test our proposed method is working well or not by using system modeling. System modeling refers to an act of representing an actual system in a simply way.

System modeling is extremely important in system design and development, since it gives an idea of how the system would perform if actually implemented.

What does security mean?

Ability for [two] nodes to effectively communicate even in the presence of active adversaries in the network

- Ability to find routes
- Availability of service
- If an “honest” path exists

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. The networks are computer networks, both public and private, that are used every day to conduct transactions and communications among businesses, government agencies and individuals.

The networks are comprised of "nodes", which are "client" terminals (individual user PCs), and one or more "servers" and/or "host" computers. They are linked by communication systems, some of which might be private, such as within a company and others which might be open to public access. The obvious example of a network system that is open to public access is the Internet, but many private networks also utilize publicly-accessible communications. Today, most companies' host computers can be accessed by their employees whether in their offices over a private communications network, or from their homes or hotel rooms while on the road through normal telephone lines.

Network security involves all activities that organizations, enterprises, and institutions undertake to protect the value and ongoing usability of assets and the integrity and continuity of operations. An effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

DOI 10.17148/IJIREEICE.2015.31220

II. LITERATURE SURVEY

1) ***On Flow Correlation Attacks and Countermeasures in Mix Networks---->*** Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao.

–In this paper, author focus on a particular class of traffic analysis attack, flow correlation attacks, by which an adversary attempts to analyze the network traffic and correlate the traffic of a flow over an input link at a mix with that over an output link of the same mix.

Pros and cons:

Analyzing of mix networks was done in terms of their effectiveness in providing anonymity and quality-of-service and it shows that it can achieve a guaranteed low detection rate while maintaining high throughput for normal payload traffic but unlinkability alone is not enough in hostile environments like battlefields as important information like packet type is still available to attackers. Then a passive attacker can mount traffic analysis based on packet type.

2) ***Anonymous Communications in Mobile Ad Hoc Networks--->*** Yanchao Zhang, Wei Liu and Wenjing Lou.

–In this paper, author proposes a novel anonymous on-demand routing protocol, termed MASK, to enable anonymous communications thereby thwarting possible traffic analysis attacks. Based on a new cryptographic concept called pairing, he first 0propose an anonymous neighborhood authentication protocol which allows neighboring nodes to authenticate each other without revealing their identities.

Pros and cons:

A pairing-based anonymous on-demand routing protocol MASK is which provides strong sender and receiver anonymity, the relationship anonymity between senders and receivers, the unlocatability of mobile nodes, and the untraceability of packet flows under a rather strong adversarial model but the routing information is not authenticated in the current design of MASK.

3) ***Self-Organized Public-Key Management for Mobile Ad Hoc Networks--->*** Srdjan Capkun , Levente Butty´ n and Jean-Pierre Hubaux.

–In this paper, author proposes a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates and to perform authentication regardless of the network partitions and without any centralized services. Furthermore, this approach does not require any trusted authority, not even in the system initialization phase.

Pros and cons:

self-organized public-key management scheme is proposed that does not rely on any trusted authority or fixed server, not even in the initialization phase. Author showed that with a simple local repository construction algorithm and a small communication overhead, this system achieves high performance on a wide range of certificate graphs but it requires users' conscious involvement only when their public/private key pairs are created and for issuing and revoking certificates.

4) ***ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks--->*** Jiejun Kong, Xiaoyan Hong.

–In this paper, author develop an untraceable routes or packet flows in an on-demand routing environment. This goal is very different from other related routing security problems such as resistance to route disruption or prevention of denial-of-service attacks.

Pros and cons:

An anonymous on-demand routing protocol ANODR for mobile ad hoc networks deployed in hostile environments. It demonstrates that untraceable data forwarding without encrypted routing header can be efficiently realized but main disadvantage of this mechanism is that all nodes receiving the RREQ message must try to decrypt the global trapdoor to find out whether it is the intended receiver, resulting in considerable overhead.

5) ***Anonymous Secure Routing in Mobile Ad-Hoc Networks--->*** Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng.

–In this paper, author proposes an Anonymous Secure Routing (ASR) protocol that can provide additional properties on anonymity, i.e. Identity Anonymity and Strong Location Privacy, and at the same time ensure the security of discovered routes against various passive and active attacks.

Pros and cons:

The Anonymous Secure Routing (ASR) protocol is proposed which provides more anonymity and security to the mobile ad-hoc networks which was a drawback in previous protocols but in the cases of route changes or link failures some problems will arise in this protocol.

6) ***ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks--->*** Stefaan Seys and Bart Preneel.

–In this paper, author present a novel anonymous on demand routing scheme for MANETs and identify a number of problems of previously proposed works and propose an efficient solution that provides anonymity in a stronger adversary model.

Pros and cons:

ARM is an anonymous on demand routing scheme for MANETs. In this author first identified a number of problems and strengths in previously proposed solutions and proposed a solution that provides stronger anonymity properties while also solving some of the efficiency problems but the computations are more in this protocol.

7) ***SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks--->*** Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba.

–In this paper, author proposes a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate node.

Pros and cons:
SDAR is an novel secure distributed anonymous routing protocol for MANET. Author discussed the protocol and highlighted its main features, which include
(i) Non-source-based routing
(ii) Flexible and reliable route selection, and
(iii) Resilience against path hijacking.

This SDAR use long-term public/private key pairs at each node for anonymous communication. These schemes are more scalable to network size, but require more computation effort.

8) ***ALARM: Anonymous Location-Aided Routing in Suspicious MANETs--->*** Karim El Defrawy and Gene Tsudik.

–In this paper, author addresses some interesting issues arising in MANETs by designing an anonymous routing framework (ALARM). It uses nodes current locations to construct a secure MANET map. Based on the current map, each node can decide which other nodes it wants to communicate with.

Pros and cons:
The ALARM framework is constructed which supports anonymous location-based routing in certain types of suspicious MANETS and it shows that that node privacy under this framework is preserved even if a portion of the nodes are stationary, or if the speed of movement is not very high but it mainly relies on group signature.

9) ***Identity-Based Encryption from the Weil Pairing--->*** Dan Boneh, Matthew Franklin.

–In this paper, author propose a fully functional identity-based encryption scheme. The performance of the system is comparable to the performance of ElGamal encryption. The security of the system is based on a natural analogue of the computational Diffie-Hellman assumption.

Pros and cons:
A ciphertext security for identity-based systems is designed and proposed a fully functional IBE system. The system has chosen ciphertext security in the random oracle model assuming BDH, a natural analogue of the computational Diffie-Hellman problem but the attacker have some negligible advantage in defeating the semantic security of the system.

10) ***SybilGuard: Defending Against Sybil Attacks via Social Networks--->*** Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman.

–In this paper, author presents SybilGuard, a novel protocol for limiting the corruptive influences of sybil attacks. This protocol is based on the "social network" among user identities, where an edge between two identities indicates a human-established trust relationship.

Pros and cons:
SybilGuard, a novel protocol for limiting the corruptive influences of sybil attacks is proposed, which is mainly used for reducing the sybil attacks of the adversaries on the networks and to provide security to the network but it mainly relies on properties of the users.

III. SYSTEM ANALYSIS

Existing system:

- A number of secure routing schemes have been brought forward
- MASK is based on a special type of public key crypto system, the pairing-based cryptosystem, to achieve anonymous communication in MANET.

Disadvantages:

Existing schemes fail to protect all content of packets from attackers, so that the attacker can obtain information like packet type and sequence number etc. This information can be used to relate two packets, which break unlink ability and may lead to source trace back attacks.

Another drawback of most previous schemes is that they rely heavily on public key cryptography, and thus incur a very high computation overhead.

Proposed system:

In this project, we introduce an efficient privacy maintain routing protocol that achieves content unobservability by employing anonymous key establishment based on group signature. The setup of this method is simple: each node only has to obtain a group signature signing key and an ID-based private key from an offline key server.

Advantages:
This project is implementing high security data transfer so we can avoid hacking unlike data security, it providing the basic packet security also.

Project description

Earlier a number of schemes have been proposed to protect privacy in Adhoc networks. However, none of these schemes offer complete unlinkability or unobservability property since data packets and control packets are still linkable and distinguishable in these schemes.

-Anonymity is the state of being not identifiable within a set of subjects, the anonymity set.

-Unlinkability of two or more IOIs means these IOIs are no more or no less related from the attacker's view.

-Unobservability of an IOI is the state that whether it exists or not is indistinguishable to all unrelated subjects, and subjects related to this IOI are anonymous to all other related subjects.

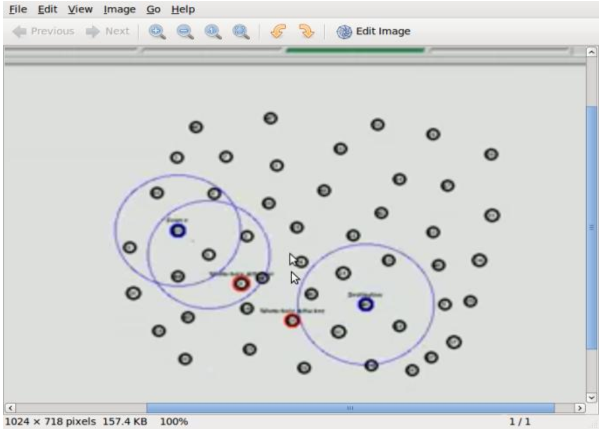
So Author defined stronger privacy requirements regarding privacy-preserving routing in mobile ad hoc networks. Then we propose an secure routing scheme to offer complete unlink ability and content unobservability for all types of packets.

The simulation results show that it not only has satisfactory performance compared to AODV, but also achieves stronger privacy protection than existing schemes.

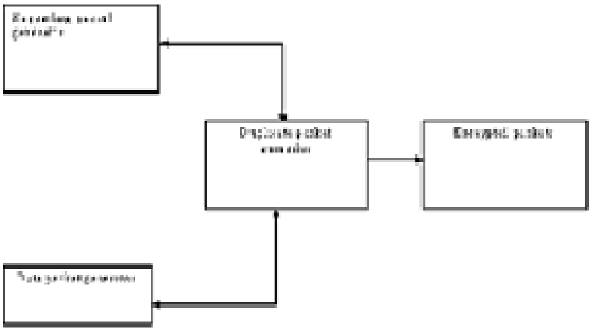
In this protocol, both control packets and data packets look random and indistinguishable from dummy packets for outside adversaries. Only valid nodes can distinguish

DOI 10.17148/IJIREEICE.2015.31220

routing packets and data packets from dummy traffic with inexpensive symmetric decryption.



Block diagram:



IV. MODULES

- Basic routing module
- Include hacking in basic routing module
- Protection against hacking

BASIC ROUTING MODULE:

- If the source has no route to the destination , then source v initiates the route discovery in an on-demand fashion
- After generating RREQ, node looks up its own neighbor table to find if it has any closer neighbor node toward the destination node.
- If a closer neighbor node is available, the RREQ packet is forwarded to that node.
- If no closer neighbor node is the RREQ packet is flooded to all neighbor nodes.

INCLUDE HACKING in basic routing module:

In this module Attack issues will arise in to the network. Providing security to the attacks will be considered.

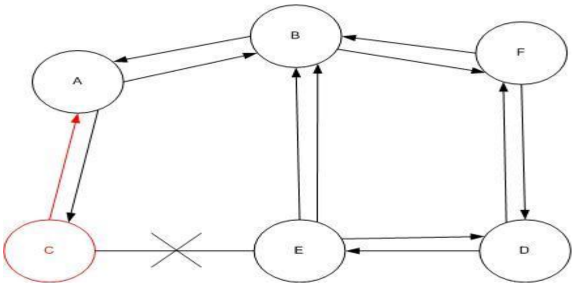
Black hole Attack:

MANETs face different securities threats i.e. attack that are carried out against them to disrupt the normal performance of the networks. In these attacks, black hole attack is that kind of attack which occurs in Mobile Ad-Hoc networks (MANET).

In black hole attack, a malicious node uses its routing protocol in order to advertise itself for having the shortest path to the destination node or to the packet it wants to intercept. This hostile node advertises its availability of fresh routes irrespective of checking its routing table. In this way attacker node will always have the availability in replying to the route request and thus intercept the data packet and retain it.

Here node "A" want to send data packets to node "D" and initiate the route discovery process. So if node "C" is a malicious node then it will claim that it has active route to the specified destination as soon as it receives RREQ packets. It will then send the response to node "A" before any other node. In this way node "A" will think that this is the active route and thus active route discovery is complete. Node "A" will ignore all other rep*lies and* will start seeding data packets to node "C". In this way all the data packet will be lost consumed or lost.

Blackhole Problem:



PROTECTION AGAINST HACKING:

In this module Group signature is taken in to consideration for the protection against hacking. Whenever node having the group id/signature then that node can interact with the other nodes in the network otherwise it cannot interact. In this way the process of avoiding the interaction of hacking node proceeds.

V. CONCLUSION

With reference to above details it is possible to overcome from weaknesses of previous intrusion detection system by sharing group IDs initially. It can be shown by comparing the quality of service parameter like routing overhead packet delivery ratio with previous IDs technique and security can be provided by using RSA.

REFERENCES

1) ARM: Anonymous Routing Protocol for Mobile Ad hoc Networks---> Stefaan Seys and Bart Preneel.
2) SDAR: A Secure Distributed Anonymous Routing Protocol for Wireless and Mobile Ad Hoc Networks---> Azzedine Boukerche, Khalil El-Khatib, Li Xu, Larry Korba.
3) ALARM: Anonymous Location-Aided Routing in Suspicious MANETs---> Karim El Defrawy and Gene Tsudik
4) Identity-Based Encryption from the Weil Pairing---> Dan Boneh, Matthew Franklin.
5) SybilGuard: Defending Against Sybil Attacks via Social Networks---> Haifeng Yu, Michael Kaminsky, Phillip B. Gibbons, Abraham Flaxman.
6) On Flow Correlation Attacks and Countermeasures in Mix Networks----> Ye Zhu, Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao.
7) Anonymous Communications in Mobile Ad Hoc Networks---> Yanchao Zhang, Wei Liu and Wenjing Lou.
8) Self-Organized Public-Key Management for Mobile Ad Hoc Networks---> Srdjan Capkun, Levente Butty´n and Jean-Pierre Hubaux.
9) ANODR: ANonymous On Demand Routing with Untraceable Routes for Mobile Ad-hoc Networks---> Jiejun Kong, Xiaoyan Hong.
10) Anonymous Secure Routing in Mobile Ad-Hoc Networks---> Bo Zhu, Zhiguo Wan, Mohan S. Kankanhalli, Feng Bao, Robert H. Deng.

DOI 10.17148/IJIREEICE.2015.31220